OmniAccess
Wireless LAN Switching Systems

The Next Generation of Wireless LAN Connectivity

Secure mobility for the enterprise

ALCATEL

Alcatel OmniAccess WLAN switching system changes how 802.11 networks are deployed, secured, and managed. Alcatel OmniAccess WLAN switching centralizes all wireless security and value-added wireless services into a single, highly resilient and scalable processing platform. Alcatel offers the most scalable WLAN systems in the industry with a unique chassis-based WLAN switch that can manage up to 512 access points (APs). Now administrators are relieved of the costly and time-consuming process of managing individual APs. And, as new security standards change and wireless services emerge, they are easily implemented at the switch and propagated throughout the enterprise.

All Alcatel OmniAccess WLAN switches combine powerful packet processing with…

- **10/100/1000 Mbps Ethernet switching**
- **stateful firewalling**
- **VPN termination**
- **wireless intrusion prevention**
- **advanced RF management**

…all within a single wireless system. Enterprises now have visibility of and remote control over the RF environment as never before because Alcatel OmniAccess WLAN switches accept and process native 802.11 traffic. Every device in Alcatel's OmniAccess WLAN switching system supports the Alcatel Operating System Wireless (AOS-W) software and integrate seamlessly into any existing wired network without having to reconfigure logical or physical devices.

FEATURES

Complete Multi-layered Security

- **RF security with integrated 802.11 IDS protects against known wireless attacks**
- **Automatic rogue AP detection and containment**
- **Unique classification of APs and stations enables automatic policy-based response**
- **L2 security with 802.1x and WPA, AES, TKIP and dynamic WEP**
- **L3 security with IPSec and PPTP VPNs**
- **Identity-based stateful firewall enables per-user security and control**
- **Role-based VLANs and SSID-based VLANs for segmenting users and traffic types**
- **Secure guest access with integrated Web-based authentication over SSL**

Wireless LAN Switching Systems

Centralized Wireless LAN Switching

- Supports IP-attached thin AP architecture enabling centralized configuration and eliminating the creation of dedicated VLANs for APs and WLAN users at the wiring closet.
- Third-party AP support
- Standards-based GRE tunneling between Alcatel switches and APs keeps WLAN traffic isolated from wired network traffic
- Programmable platform allows easy deployment of upgrades and new wireless applications

Advanced RF Management

- Integrated RF plan software allows modeling, planning and placement of APs
- Centralized and distributed calibration automates AP deployment and provides optimal coverage through optimum power and channel tuning
- Self-healing capabilities for APs and AP-to-switch connectivity minimizes network downtime
- Load balancing distributes users across multiple APs
- Interference detection and coverage hole detection

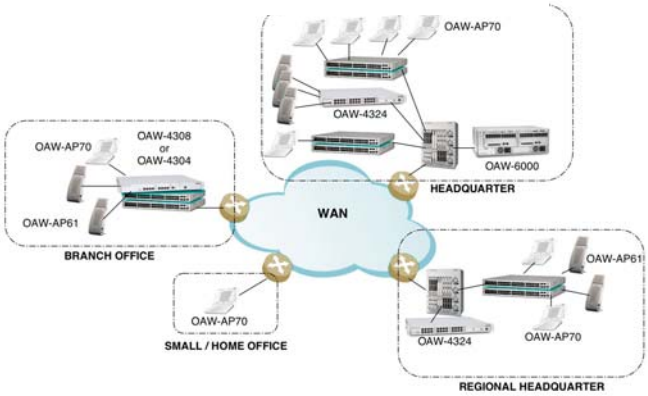
Standards-based Enterprise Mobility

- Mobile IP technology for secure enterprise-wide mobility across different subnets, APs, and switches
- Fast roaming (typically 2-3 msec) allows mobility for all users and applications
- Proxy mobile IP eliminates client software requirement for transparent mobility
- Proxy DHCP enables VPN tunnel persistence as user roams across subnets

QoS for Latency-sensitive Applications

- Fast handoffs between APs for VoIP mobility
- Multiple queues over the air
- Stateful-flow classification for prioritization of VoIP and streaming media
- Bandwidth contracts to enforce usage limits
- 802.1p/DiffServ support for prioritizing traffic across the wired and wireless networks

Flexible Deployment Options



Transparent AP-to-Switch Connectivity

There is no need to create new VLANs and IP subnets in every wiring closet switch for wireless APs and users because Alcatel OmniAccess Access Points uniquely forward 802.11 traffic to Alcatel OmniAccess WLAN switches across any L2/L3 wired network using standard generic routing encapsulation (GRE) tunnels. Wireless VLANs only need to be created inside the centralized WLAN switches for segmenting 802.11 traffic according to user roles and SSIDs.

Centralized Wireless Security Protects the Air, the Data, the Network, and the User

Alcatel OmniAccess WLAN switching system uniquely delivers multi-layered wireless security that protects the air, the data, the network, and the users. A patented classification engine coupled with sophisticated RF monitoring lets administrators protect the air by automatically detecting unauthorized users, containing rogue APs and ensuring users don't associate with interfering APs. Link layer security, with support for WEP, dynamic WEP, TKIP (WPA 1.0), and AES protects user data.

Port-based 802.1x authentication is used with standard authentication mechanisms such as RADIUS, LDAP, or Active Directory, and combined with link layer encryption to ensure user privacy. Network layer security lets enterprises terminate IPSec VPN tunnels at LAN speeds inside the corporate intranet. An integrated firewall lets administrators create and enforce stateful policies that follow users.

Secure Mobility

The Alcatel OmniAccess WLAN switches give users of wireless laptops, PDAs, and other 802.11 mobile devices secure access while moving within and between campus buildings and corporate subnets. With an integrated stateful firewall that can be applied on a per-user basis, administrators establish unique access, service, and security policies for different users or user groups. Policies are based on any combination of parameters such as user, group, duration, time-of-day and location. These policies are centrally configured and propagated throughout the network so administrators can enforce desired levels of security and QoS for users as they move.

L2 and L3 mobility between APs, subnets, and WLAN switches using proxy DHCP and proxy mobile IP eliminates lost sessions and the need for users to re-authenticate. No mobile IP software is required on client stations.

Authentication and Access Control

The Alcatel OmniAccess WLAN switches support MAC and IP based user authentication methods including the IEEE 802.1x framework that allows the use of PEAP, EAP-TLS, and EAP-TTLS with RADIUS, and IPSec VPNs using PPP or L2TP with CHAP or MS-CHAP. In addition, users can be authenticated against existing LDAP, RADIUS, or Windows domain servers as well as a local database inside the Alcatel OmniAccess WLAN switch.

User and role-based access control allows specific user policies to be defined. Browser-based authentication allows differentiated class-of-service through secure HTTPS or SSL.

Plug and Play Deployment

The Alcatel OmniAccess WLAN switches can be centrally deployed without having to directly connect access points. Each WLAN switch stores the configuration of each Alcatel AP. When a new Alcatel AP is connected to the system, it is automatically discovered and configured by the switch. Alcatel OmniAccess WLAN switching provides complete control of the power and channel settings of each attached AP and is the only solution to deliver Ethernet, console, and power over a single CAT 5 cable to any Alcatel or third-party AP.

Advance Wireless Capabilities

Alcatel OmniAccess WLAN switching technology now gives administrators advanced wireless features. These capabilities include setting bandwidth contracts to limit low priority users, classifying and prioritizing traffic flows to support delay-sensitive applications such as VoIP and automating VLAN membership through roles derived from backend authentication systems that leverage 802.1x, captive portal, or VPN authentication methods.

Single Point for Global Management

Multiple Alcatel OmniAccess WLAN switches distributed in branch or regional offices can be centrally managed from a master Alcatel OmniAccess WLAN switch. All switch configuration and user policies can be defined from the master switch and automatically propagated to Alcatel OmniAccess WLAN switches in remote locations. From a master Alcatel OmniAccess WLAN switch, administrators can manage, secure and control branch office RF environments, capture wireless traffic, and remotely troubleshoot problems.

Alcatel OmniAccess WLAN switches are managed via a Web-based graphical user interface or command line interface and provide full support for SNMP (v3).

The Alcatel OmniAccess WLAN switches are integrated within Alcatel's OmniVista Enterprise network management application. OmniVista discovery and topology applications enable a network administrator to view both wired and wireless network elements and topologies from a single screen. OmniVista also provides the network administrator with the ability to seamlessly launch the OmniAccess WLAN manager application.

The Alcatel OmniAccess WLAN switches can also be easily integrated into third-party management systems such as HP OpenView or Computer Associate's Unicenter.

Alcatel Next Generation Wi-Fi Switching Product Family

Alcatel OmniAccess 6000

The four-slot Alcatel OmniAccess 6000 (OAW-6000) WLAN switch supports up to 72 10/100 Mbps Ethernet (RJ-45) user ports and six Gigabit (GBIC) uplinks. Hot swappable components include a 24 port 10/100 Mbps Ethernet line card, supervisor modules, fan tray, and up to three power supplies. It offers Power over Ethernet, two GBIC ports as well as tri-color AP LEDs. A supervisor module integrates a hardware encryption engine capable of delivering up to 7.2 Gbps of encrypted traffic.

Alcatel OmniAccess 4324

The Alcatel OmniAccess 4324 (OAW-4324) is a stackable, 24-port WLAN switch that supports up to 48 APs and also functions as an appliance. Designed for regional headquarters or dense building deployments, the OAW-4324 supports up to 512 simultaneous users and delivers up to 400 Mbps of encrypted throughput.

Alcatel OmniAccess 4308

The Alcatel OmniAccess 4308 (OAW-4308) is a fixed configuration WLAN switch designed for remote and branch office applications. The Alcatel OAW-4308 provides eight 10/100 Mbps user ports, one copper gigabit uplink and an expansion slot to support a fiber gigabit connection. Programmable hardware-based encryption supports 200 Mbps of full-duplex encrypted traffic.

Alcatel OmniAccess AP60 and AP61

The Alcatel OmniAccess AP60 and AP61 (OAW-AP60 and OAW-AP61) are single radio, 802.11a or b/g access points (APs) designed for dense wireless deployments. The Alcatel OAW-AP60 and OAW-AP61 deliver superior capacity, performance, and coverage.

Alcatel OmniAccess AP70

The Alcatel OmniAccess AP70 (OAW-AP70) is a dual-radio access point that provides concurrent operation of 802.11a and 802.11b/g services. The OAW-AP70 is a multi-purpose device that can function both as an access point and as an RF monitor – independently or concurrently – across the 2.4 GHz and 5 GHz spectrums. Ideally suited for workspace deployment, the OAW-AP70 can be securely wall or desk-mounted.

Alcatel Operating System – Wireless (AOS-W)

Alcatel's AOS-W software comes standard on all Alcatel WLAN switching systems. AOS-W based features include: L2/L3 switching (port mirroring, Ether channel, static routes, ACLs, STP active/active VRRP redundancy between switches), and VoIP-grade mobility.

Wireless LAN Switching Systems

Alcatel's AOS-W RF management application provides full-featured WLAN switching functionality – adding advanced features such as virtual wireless LANs, RF spectrum management, automatic calibration, load balancing, and interference detection.

Alcatel's AOS-W Wireless IDS application provides patented classification technology that helps to proactively protect against malicious attacks as well as client and station impersonations, such as de-auth and probe request floods, man-in-in-the middle, and ASLEAP attacks.

Alcatel's AOS-W Firewall application gives administrators the power to provide advanced security for any AP such as enforcing stateful firewall policies per user or per port, stateful user identification through 802.1X or Windows login, and role-based access controls.

Features & Benefits

- **Multi-layered (L1, L2, L3 and L4-7) security**
  Simultaneously protects RF, data, network and users
- **Wireless IDS**
  Proactively protects against malicious attacks and station and AP impersonations
- **Identity-based stateful firewall**
  Allows firewall policies to be created on a per user basis and enforced as each user roams
- **System resilience and redundancy**
  High system availability. Auto failover between switches using VRRP. Auto failover of APs. Modularity and redundancy among all system components
- **Centralized encryption**
  One simple upgrade at switch for entire system, data encrypted across the network
- **Patented classification engine**
  Automatically classifies and validates users and devices on network. Stations, APs, and devices are classified as valid, rogue, or interfering
- **Advanced RF monitoring**
  Gives IT staff visibility and control of entire 802.11 environment from a single point
- **Integrated hardware-based encryption**
  Eliminates time-consuming upgrades, delivers from hundreds of megabits to gigabits of encrypted throughput on a single system
- **Flow classification**
  VoIP or other delay sensitive traffic classified and prioritized over the air and wire
- **Interference detection**
  Pinpoint interfering RF sources from a single point
- **Backbone (indirect) connect**
  Centralized deployment within backbone with no physical or logical reconfiguration, APs attached to existing wired switches
- **Wireless RMON and remote packet capture/analysis**
  No overlay networks required for remote wireless troubleshooting, on demand access to wireless traffic statistics, centralized packet analysis
- **Bandwidth contracts**
  Enforce per user limits on bandwidth consumption
- **Seamless and secure mobility**
  Eliminates lost sessions and need for users to re-authenticate. Allows secure and transparent user mobility across different subnets, APs and switches, eliminates client software, keeps VPN tunnel state
- **Role-based and SSID-based VLANs**
  Automatically places users and traffic into correct VLAN using existing wired VLAN assignments. Segments different users and traffic types over single wireless infrastructure
- **RF Planning with auto calibration**
  Obviates need for expensive site surveys, eases deployment effort, provides optimal coverage on an on-going basis

www.alcatel.com/enterprise

Alcatel

26801 West Agoura Road
Calabasas, CA 91301 USA

Contact Center
(800) 995-2612 US/Canada
(818) 880-3500 Outside US

www.alcatel.com/enterprise

Product specifications contained in this document are subject to change without notice. Contact your local Alcatel representative for the most current information. Copyright © 2005 Alcatel Internetworking, Inc. All rights reserved. This document may not be reproduced in whole or in part without the expressed written permission of Alcatel Internetworking, Inc. Alcatel® and the Alcatel logo are registered trademarks of Alcatel. All other trademarks are the property of their respective owners.

P/N 031668-00 05/05

ALCATEL